HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

BENNETT HASELTON, an individual; PEACEFIRE, INC., a Washington corporation Plaintiff, vs. QUICKEN LOANS, INC., a Michigan corporation; and JOHN DOES, I-X Defendant.	)	CIVIL ACTION NO. C07-1777 RSL **DECLARATION OF STEPHANIE L. STRIKE IN SUPPORT OF OPPOSITION TO PLAINTIFFS' MOTION FOR PROTECTIVE ORDER AND FOR PARTIAL SUMMARY JUDGMENT RE STANDING**

I, Stephanie L. Strike, hereby declare:

1. I am over the age of 18 and have personal knowledge of the facts described herein.

2. I am one of the attorneys representing Defendant Quicken Loans, Inc. in this matter.

3. Attached hereto as Exhibit A is a true and correct copy of information I printed from the Peacefire.org website on May 13, 2008.

4. Attached hereto as Exhibit B is a true and correct copy of an excerpt from Defendant's first set of discovery requests and Plaintiffs' responses thereto.

5. Attached hereto as Exhibit C is a true and correct copy of information I printed from various websites defining "IAP" and "ISP" which returned as results to my query on Google.com with search terms "IAP" or "ISP" or "IAS" on May 10, 2008.

6. Attached hereto as Exhibit D is a true and correct copy of information I printed from the Washington Courts website on May 13, 2008.

7. Attached hereto as Exhibit E is a true and correct copy of a document produced by Plaintiffs that appears to be an invoice from their alleged Internet access service, JVDS.

8. Attached hereto as Exhibit F is a true and correct copy of Plaintiffs' FRCP 26 Initial Disclosures.

I hereby certify pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct.

Signed this 19th day of May, 2008 at Seattle, Washington.

/s/ Stephanie L. Strike
STEPHANIE L. STRIKE

CERTIFICATE OF SERVICE

I hereby certify that on this date I filed the foregoing with the United States District Clerk, Western District of Washington at Seattle, using the ECF filing system, which sent an email notification of this filing to the below-listed counsel of record:

Robert J. Siegel bob@ijusticelaw.com	**Douglas E. McKinley** doug@mckinleylaw.com

Dated this 19th day of May, 2008.

/s/ Michelle F. Hall
Michelle F. Hall

Exhibit A

PEACEFIRE
Open Access for the Net Generation

Blocking Software Reports

BESS
Cyber Patrol
WebSENSE
Net Nanny
SmartFilter
X-Stop / 8e6
I-Gear
CYBERsitter

About Peacefire
Join Peacefire
Blocking Software FAQ
Contact
Press information

webmaster@
peacefire.org

How to disable your blocking software | Why we do this
You'll understand when you're younger
About Peacefire | Join Peacefire | Blocking Software FAQ | Contact us |
Press information

To get around your blocking software: 中文

- **1. First, try a circumvention site like https://www.StupidCensorship.com/.** Be sure to type **https** at the beginning of the URL, not 'http'. Even though this site has been widely known for months, many networks have their blocking software set up incorrectly so that sites beginning with **https://** are not blocked, and https://www.StupidCensorship.com/ will still be accessible.

- **2. If that doesn't work, you can join our e-mail list where we mail out new Circumventor sites every 3 or 4 days.** Of course, employees of blocking software companies have gotten on this list as well, so they add our sites to their blocked-site database as soon as we mail them out, but in most places it takes 3-4 days for the blocked-site list to be updated. So the latest one that we mail out, should usually still work.

- **3. If you have a computer with an uncensored Internet connection, you can follow these easy steps to set up your own Circumventor site.** For example, if you want to get around blocking software at work, and you have a home computer with an uncensored Internet connection, you can install the Circumventor on your home computer. Then it will give you a new URL, and you can take that URL in with you to work and type it into your browser to get around the network blocking software.

- **4. If you're trying to get around blocking software that's installed on the local computer, and not on the network, use these instructions to boot from the Ubuntu Live CD.** (These instructions include tips on how to tell the difference between blocking software that's installed "on the local computer" and software that's installed "on the network".)

Install the Circumventor
Is StupidCensorship.com already blocked for you because it's been widely known for so long? This is how you create your own semi-private URL for getting around blocking software.

Highlights reel

Past news items that generated the most interest:

Report on double standards for anti-gay "hate speech"
Peacefire created four pages, on free servers such as GeoCities, which consisted of anti-gay quotes copied from four different conservative Web sites: Dr. Laura, Concerned Women for America, Family Research Council and Focus on the Family. Using anonymous HotMail accounts, we then sent the URLs of the newly created pages to six blocking software companies, recommending that they block the newly created pages as "hate speech". After the companies had agreed to block the sites we created, we told them that all the quotes on those pages had been taken from the four conservative Web sites, and recommended that they block those Web sites as well. The blocking companies did not block those Web sites and did not respond to our inquiries.

WebSENSE publishing daily porn links
For five months, the makers of WebSENSE blocking software published a daily list of pornographic Web sites that were not blocked by their competitors, allegedly to show that their own product was superior. Students using the Internet in schools that were using those competitors' products, could access the WebSENSE site and get a list of unblocked porn sites, by clicking a link agreeing that they were over 18 years of age.

Human rights pages blocked
In December 2000, Peacefire released Amnesty Intercepted, a report on human rights pages including Amnesty International that were blocked by blocking software.

Candidates' sites blocked during 2000 elections
In November 2000, Peacefire released a list of political candidates whose sites had been blocked as "pornography" by major blocking programs. One candidate had carried the statement on his Web site, "We should demand that all public schools and libraries install and configure Internet Filters." He changed his position after finding out that his own site was blocked, and later became a plaintiff in the ACLU's lawsuit to overturn a law requiring blocking software in schools and libraries.

Pro-blocking site blocked
In July 1997, librarian David Burt launched the now-

defunct FilteringFacts.org site, advocating the use of blocking software in libraries. The site was later blocked as a "Drugs/Alcohol" site by SurfWatch (which has since been bought out by Cyber Patrol).

Off-site research links

- Ben Edelman's reports, used as evidence in the ACLU's legal challenge to a law requiring blocking software in schools and libraries, discuss the large numbers of sites classified inaccurately by blocking software.
- Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet. From the Electronic Privacy Information Center.
- Internet Filters: A Public Policy Report, from the Free Expression Policy Project
- Two reports from the Gay and Lesbian Alliance Against Defamation -- Access Denied, released in December 1997, and Access Denied 2.0, released in March 2000 -- discuss targeting of non-pornographic gay and lesbian Web sites by blocking software.

PEACEFIRE
Open Access for the Net Generation

Blocked Site of the Day

Blocking Software Reports

BESS
Cyber Patrol
WebSENSE
Net Nanny
SmartFilter
X-Stop / 8e6
I-Gear
CYBERsitter

About Peacefire
Join Peacefire
Blocking Software
FAQ
Contact
Press information

webmaster@
peacefire.org

Home | About Peacefire | Censorware | Contact

About Peacefire.org

"Congress shall make no law abridging the freedom of sXXXch, or the right of the people peaceably to XXXemble, and to peXXXion the government for a redress of grievances."
-- Marc Rotenberg

"You can tell this is such a great club because we always get in trouble for following our charter."
-- Calvin & Hobbes

(See also "Why we do this -- A note to people who think we suck". Please read before sending "FundaMail".)

Peacefire.org was created in August 1996 to represent the interests of people under 18 in the debate over freedom of speech on the Internet. The Web site and mailing lists are maintained by Bennett Haselton, who is now a freelance programmer in Seattle. Peacefire has about 7,000 members on our mailing list as of February 2003; you can join Peacefire and get on the mailing list at no cost. Peacefire also has about 12 staff members that run the organization.

Peacefire is a "people for young people's freedom of speech" organization, not a "young people for freedom of speech" organization. In other words, you can join at any age if you are against censorship for students and people under 18 in general. Peacefire used to be more of a "teens only" group, but we realized that there was no point in excluding what any potential members had to offer, simply based on their age.

The first content to appear on Peacefire.org consisted of lists of some of the Web sites that were blocked by popular censorware programs such as Cyber Patrol and CYBERsitter. Since then, the information on Peacefire.org has been used by lawyers for the American Civil Liberties Union, People For the American Way, and other anti-censorship groups to challenge Internet censorship laws in Congress and in several state legislatures. Since we cannot afford our own lobbyists or legal campaigns, our most useful contribution is to provide facts and research which is then used by larger organizations that *can* afford their own lawyers.

In October 1998, we added pages to Peacefire.org about how to disable the different censorware programs. The censorware-disabling instructions were linked from a page titled "WINnocence: Innocence-preserving software for Windows", a blocking software parody that was later taken down because many people thought it was not a joke. The original WINnocence parody page is here.

Since Peacefire was created, staff members have been invited to speak about blocking software at the American Library Association National Conference, the ACLU of Ohio annual meeting, the Maine Library Association annual conference, Computers, Freedom and Privacy, and Spring Internet World '99. Members have also been interviewed about Internet censorship on television on MSNBC, MTV, Court TV and CNN Financial News.

Peacefire first received attention in December 1996 when CYBERsitter added it to their list of "pornographic" Web sites and sent a letter to our ISP threatening to block all of their hosted sites if Peacefire were not closed down. Wired News ran a story about the controversy which was picked up by PointCast and some other news services. The usual response from people who hear about this now is, "Of course CYBERsitter blocked their site -- they have pages about how to turn the program off!" Actually, we didn't add information about how to disable CYBERsitter (and other programs) to Peacefire.org until October 1998, which is why it generated so much controversy when CYBERsitter blocked our site in 1996. The only content on Peacefire.org at that time that had anything to do with CYBERsitter was our original CYBERsitter page, which listed some of the Web sites that the program blocked, including N.O.W., Mother Jones and the International Gay and Lesbian Human Rights Commission.

Bennett Haselton is a freelance programmer in Seattle and can be reached at bennett@peacefire.org or (425) 497 9002.

PEACEFIRE
Open Access for the Net Generation

Home | About Peacefire | Censorware | Contact

You can join Peacefire by filling in your e-mail address in the space below and clicking "Subscribe". Members will be automatically signed up to receive a newsletter from Peacefire, sent out about once a week.

Subscribe

Peacefire keeps all information about its members confidential. Your e-mail address will never be sold or given away to anyone, and all messages from Peacefire will include instructions on how to unsubscribe from the mailing list.

Blocked Site of the Day

Blocking Software Reports

BESS
Cyber Patrol
WebSENSE
Net Nanny
SmartFilter
X-Stop / 8e6
I-Gear
CYBERsitter

About Peacefire
Join Peacefire
Blocking Software FAQ
Contact
Press information

webmaster@peacefire.org

Blocking Software FAQ

1. What kind of sites are blocked by the different blocking programs?
2. How can I get a list of sites blocked by a given censorware program?
3. I heard that a site was blocked by a particular program, but when I tested the program, it said that the site was not blocked. What happened?
4. How can I find out if my site is blocked by any of the programs?
5. Why is it that "keyword blocking" cannot really be turned off?

What kind of sites are blocked by the different blocking programs?
A: The controversy over blocking software does not center on the blocking of chicken breast recipes, breast cancer information, Anne Sexton, or "Superbowl XXX". It is true that these sites are *accidentally* blocked by blocking software programs that scan pages for certain keywords, as almost all of them do. However, the controversy centers on sites that are blocked not accidentally but deliberately. These are URL's that come pre-included on the list of sites to be blocked by the program, regardless of the content of the pages themselves. Some examples:

- CYBERsitter blocked *TIME* Magazine as a result of an article that criticized CYBERsitter's blocking policies (this article is no longer online). *TIME* published a follow-up article about their site getting blocked: CYBERsitter Decides To Take A Time Out (currently only available through the Internet Archive)
- Cyber Patrol blocks the Envirolink animal rights Web site, because the manufacturer determined that Envirolink's descriptions of animal testing in laboratories were inappropriate for children. Cyber Patrol was also discovered to be blocking the Ontario Center for Religious Tolerance at one point. A report from the non-profit Censorware Project listed dozens of additional sites that were blocked by Cyber Patrol.
- An ACLU position paper reported that BESS, which controls Internet access used by about 3 million students in the U.S., blocked the anti-racist HateWatch Web site and the Marijuana Policy Project, a page that advocates the use of medical marijuana.
- The X-Stop Files, an essay published in October 1997 by attorney Jonathan Wallace, named some of the sites that were hard-coded on X-Stop's list of blocked URL's, including the AIDS Quilt and the official home page of the Quakers. Mr. Wallace was later called to testify on his findings in a First Amendment lawsuit filed by People For the American Way against a library that was using X-Stop.

Q: How can I get a list of sites blocked by a given censorware program?
A: You cannot get a list of blocked sites by downloading a trial copy of the program. Even though most censorware programs have free-trial versions that come with a copy of the blacklist, the list is stored in an encrypted file that is not supposed to be readable to the user. The only censorware program that does not encrypt their blocked site list is Net Nanny, however, their blocked site list is not available with the free trial version.

Your first option is trial and error. You can download the program and try to access different sites to see which ones are blocked. This is how Peacefire came up with lists of sites that were blocked by the different censorware programs when we examined them. You can go to http://www.peacefire.org/censorware/ and find the program on that page, for a list of some of the sites that were blocked when we tested it.

There have also been several cases where the encryption on a particular program's blacklist was broken, and the entire list of blocked sites was posted to the Internet. Peacefire broke the encryption on

CYBERsitter's blocked site list and published a program called CSDecode in April 1997 that could be used to decrypt the list of sites blocked by CYBERsitter 2.12. Anyone could get a list of sites blocked by CYBERsitter by downloading CYBERsitter, downloading our CSDecode program, and running it against CYBERsitter's list of blocked sites.
You can get the entire list of sites blocked by CYBERsitter at:
http://www.xs4all.nl/~mjk/cybersitter.html
and the entire list of sites blocked by Net Nanny at:
http://www.xs4all.nl/~mjk/netnannysites.html
(even though the Net Nanny list didn't have to be decrypted). Peacefire is not affiliated with these sites; the URL's themselves have information on how to contact the author.

In March 1997, TIME Magazine online posted a tool called the "Censorware Search Engine", created by journalists who managed to obtain decrypted copies of the blocked site lists used by Cyber Patrol, SurfWatch, Net Nanny, CYBERsitter, and X-Stop. The user could enter a keyword and the search engine would reply with a list of URL's from the different blacklists that contained that keyword. CYBERsitter added TIME magazine to their list of blocked sites, apparently in retaliation. But the Censorware Search Engine was taken permanently offline in about August 1998 during an overhaul of the TIME Digital Web site.

Q: I heard that a site was blocked by a particular program, but when I tested the program, it said that the site was not blocked. What happened?
A: The company may have removed the site from their list since it was discovered to be blocked. Even if the company has removed the site from their blacklist, all users of the program have to download the latest version of the blacklist before it will take effect on their computer. Depending on who told you that the site was blocked, it might have been that they received an error of a different kind (e.g. "404 File Not Found" or "403 Forbidden") and thought that it was caused by the blocking software.

All blocked sites listed on Peacefire.org were obtained through trial and error, by testing the latest available copy of the program's blacklist (unless -- in the case of CYBERsitter -- we were able to break the encryption on the blacklist and examine it directly). In some cases, if we were worried that the company might un-block a site after our report was published and deny that the site was ever blocked in the first place, we asked reporters to go through the list of sites and verify that they were blocked, before our page was published.

Many examples of blocked sites listed on our pages are there to demonstrate that the censorware company is not reviewing pages before blocking them, such as the Vatican site blocked by X-Stop or the Breast Cancer Legislation site blocked by BESS. Even if these pages are un-blocked after the discovery is made public, they still would not have been blocked in the first place if the sites had been reviewed by a human first.

Q: How can I find out if my site is blocked by any of the programs?
A: The following three companies have published "lookup forms" on their Web sites where you can enter the URL of your page, and the form will tell you whether it's blocked or not:

- SurfWatch used to offer a form at http://www1.surfwatch.com/testasite/ where a user could enter a URL to see if it was blocked by SurfWatch, but that site is no longer available. (Even though SurfWatch is no longer being sold, the product is still in widespread use, and existing customers still receive updates to the SurfWatch blocked-site list -- so it would be useful for SurfWatch to restore access to the "Test-A-Site" form.)
- Cyber Patrol -- CyberNOT search engine
- WebSENSE -- site lookup

- SmartFilter -- SmartFilterWhere Version 3, to look up sites according to the categories that they're blocked under in SmartFilter 3.0. (An older version of SmartFilterWhere lets you look up sites according to the categories they're blocked under, in older versions of SmartFilter.)
- N2H2 / Bess -- URL checker

Note that some of these forms may return incorrect information. For example, if a site is blocked automatically by Cyber Patrol because it has the word "sex" in the URL, the site may still be listed as "not blocked" if you enter the URL in the form on their site. To find out for sure if a program is blocking a Web site, you should download and install the software.

To find out whether your site is blocked by any other program, downloading the program and installing it is the only choice you have. Of all the companies that offer free downloads of their programs, the trial versions block all of the same sites that the full versions block (except for the trial versions of Net Nanny and WebSENSE).

Some programs -- usually proxy servers such as BESS, I-Gear and SmartFilter -- do not have trial versions that you can download, since they are for use by schools and companies but not by home users. In that case, you have to contact the company to ask them if they are blocking a Web site, or contact someone at a company or school that is using the software, and ask them to test the URL for you.

Q: Why is it that "keyword blocking" cannot really be turned off?
A: Normally, a site is blocked if (1) the URL is on the program's internally stored "blacklist" or (2) the program detects certain keywords on the page and blocks it automatically, whether the URL is on the blacklist or not. When a censorware program includes an option to "turn keyword blocking off", this means that condition (2) no longer applies, so the site will only be blocked if it's on the blacklist. Some users have wondered if the really embarrassing errors caused by blocking software -- such as blocking sites about breast cancer -- can be avoided if you disable keyword blocking.

The reason this doesn't work is because censorware companies use keywords to generate the blacklist itself. X-Stop, for example, uses a program called "MudCrawler" to search the Web for pages containing words like "xxx" in the title. As a result, sites are added to the blacklist that probably would not have been added if they had been reviewed by a human first. The Quakers home page and the AIDS Memorial Quilt were both discovered to be on X-Stop's blacklist. Cyber Patrol, which developed their own program called CyberSpider similar to X-Stop's MudCrawler, blocked a youth soccer league, MapleSoccer.org, because of a page that listed the teams in the categories "Boys under 12", "Boys under 14", etc. These sites were blocked even on computers where keyword blocking was *disabled*, because they were on the program's blacklist.

bennett@peacefire.org

PEACEFIRE
Open Access for the
Net Generation

Peacefire Contact Information

Bennett Haselton is at:
bennett@peacefire.org
(425) 497 9002

webmaster@peacefire.org

Bennett Haselton can be contacted by e-mail at bennett@peacefire.org.
For more research material:

- Please click here if you are interested in writing a **serious** article about Internet censorship issues

- Please click here if you are interested in writing a **sensationalist** article about Internet censorship issues

Resources for journalists writing serious articles

We have a list of the 2 most common mistakes when writing about blocking software. The rest of our resources are organized according to how much time you have left.

My deadline is:
A few days away An hour ago

Deadline was an hour ago
If you need a quick statement, try calling us or one of these people:

- Lawyers and policy experts that:
  - oppose Internet censorship
  - support Internet censorship
- People whose Web sites have been blocked
- Blocking software companies
- Politicians with positions on Internet censorship

(E-mail address and personal phone numbers have only been listed with the person's permission.)

Lawyers and policy experts opposing Internet censorship

Ann Beeson, American Civil Liberties Union	beeson@aclu.org	(212) 549-2500
Ann Beeson is the lawyer with the national office of the ACLU who argued successfully against the Communications Decency Act in 1996. She also co-ordinated ACLU efforts against blocking software in libraries in Kern County, CA and Loudoun County, VA.		

Jonathan Wallace, Censorware Project	jw@bway.net	(718) 797-9808
Jonathan Wallace is an attorney and software executive in Brooklyn. In 1997 he wrote "Purchase of Blocking Software by Public Libraries is Unconstitutional, the first online paper about the legality of Internet censorship in libraries. In October 1997 he published The X-Stop Files, an analysis of X-Stop and some of the sites that the program blocked. Mr. Wallace later testified in *Mainstream Loudoun v. Board of Trustees*, the court case which resulted in a ruling by a federal judge that use of X-Stop blocking software in a Virginia library was a violation of the First Amendment. Mr. Wallace's own Web site, The Ethical Spectacle, was blocked at different times by X-Stop, BESS, CYBERsitter and Cyber Patrol.		
Jim Tyre, Censorware Project	jstyre@jstyre.com	(310) 839-4114
Jim Tyre is a volunteer lawyer for, and founding member of, the Censorware Project. He also defended Peacefire pro bono against CYBERsitter's threats of a lawsuit against us for publishing a program that decrypted CYBERsitter's list of blocked sites.		
Jon Katz, Marks & Katz, LLC, Attorneys at Law	jon@markskatz.com	(301) 495-4300
Jon Katz represented the Free Speech Coalition on an obscenity law panel held by the National Association of Sciences committee. In June 2001 he was elected president of the Free Speech Coalition of the District of Columbia, Maryland and Virginia. He is also a member of the First Amendment Lawyers Association and the Libel Defense Resource Center. More information on his law firm's activities can be found at http://www.markskatz.com/overview.htm (No relation to Jon Katz, the HotWired and Slashdot writer.)		

Lawyers and policy experts supporting Internet censorship

Bruce Taylor, National Law Center for Children and Families	east@nationallawcenter.org	(703) 691-4626
Bruce Taylor helped author sections of the Communications Deceny Act of 1996 and has written a long memorandum supporting the use of blocking software in libraries.		
Ken Bass, Venable Attorneys At Law	kbass@venable.com	(202) 962-4890
Ken Bass argued a court case in favor of the public library policy in Loudoun County, VA, which required all users to use X-Stop blocking software.		
Michael Millen, Pacific Justice Institute	MikeMillen@aol.com	(408) 871-0777

Michael Millen argued a lawsuit on behalf of a mother who sued the Livermore, CA public library for not installing blocking software, claiming in the lawsuit that people looking at pornography before they are 18 can result in "damage to their nervous systems".		
David Burt, Filtering Facts	webmaster@filteringfacts.org	
David Burt runs the Filtering Facts Web site, advocating the use of blocking software in libraries.		

People whose Web sites have been blocked

(Peacefire's Web site is blocked, of course, so you could also call us.)

Jonathan Wallace, The Ethical Spectacle	jw@bway.net	(718) 797-9808
Jonathan Wallace is an attorney and software executive in Brooklyn. In 1997 he wrote "Purchase of Blocking Software by Public Libraries is Unconstitutional, the first online paper about the legality of Internet censorship in libraries. In October 1997 he published The X-Stop Files, an analysis of X-Stop and some of the sites that the program blocked. Mr. Wallace later testified in *Mainstream Loudoun v. Board of Trustees*, the court case which resulted in a ruling by a federal judge that use of X-Stop blocking software in a Virginia library was a violation of the First Amendment. Mr. Wallace's own Web site, The Ethical Spectacle, was blocked at different times by X-Stop, BESS, CYBERsitter and Cyber Patrol.		
Jamie McCarthy, formerly with the Nizkor Project	jamie@mccarthy.vg	
Jamie McCarthy is the former webmaster of Nizkor.org, a Holocaust research project site which has been blocked by SmartFilter, I-Gear and Cyber Patrol. He is a founding member of the Censorware Project and wrote Blacklisted by Cyber Patrol, the Censorware Project's first report on sites blocked by Cyber Patrol.		
Josh Knauer, of Envirolink	josh@envirolink.org	(412) 420-6400
Josh Knauer founded Envirolink in 1991 when he was a college freshman. Cyber Patrol has been blocking the Envirolink Animal Rights Resource Site since 1996, because of the pictures of animal testing in the archive.		
Nels Henderson	nelsh@rain.org	
Nels Henderson is the co-webmaster of the Stop AIDS Project, which has been blocked by X-Stop and I-Gear.		
Monnica Terwilliger, maintainer of Epigee	help@epigee.org	

Monnica is the author of the Epigee Birth Control Guide, which was classified as a pornography site by BESS blocking software.		
James J. O'Donnell, Professor of Classical Studies and Chief Information Officer for the University of Pennsylvania	jod@isc.upenn.edu	(215) 898-1787
Professor O'Donnell's Internet seminar on the works of St. Augustine attracted 500 participants in 1994. His web site, which includes Augustine's home page, includes the censored file, *Aureli Augustini Confessionum liber decimus* -- the full Latin text of the 10th book of Augustine's famous *Confessions*. As best can be determined, this text was blocked because of the high frequency of the word *cum*, Latin for "with" or "when".		

Blocking software companies

SurfWatch	800-458-6600
Cyber Patrol	Susan Getgood, 617-494-5674
CYBERsitter	(800) 388-2761
X-Stop (Log On Data)	(714) 282-6111
Net Nanny	(604)662-8522
Bess (N2H2)	(800) 971-2622
SmartFilter (Secure Computing Ltd.)	(408) 918-6100
WebSENSE (NetPartners)	(800) 723-1166
I-Gear (URL Inc.)	757-865-0810

Politicians who support Internet censorship

Senator James Exon (D-NE), author of the Communications Decency Act of 1996, and Senator Dan Coats (R-OK), author of the Child Online Protection Act of 1998 ("CDA II"), have retired.

Senator John McCain (R-AZ)	John_McCain@McCain.senate.gov	(202) 224-2235
Senator McCain introduced a bill in February 1998, the "Internet School Filtering Act", that would require all public schools and libraries to install blocking software, on pain of losing all federal financial support. The bill passed the Senate but was not included in the final 1998 spending bill.		
Senator Patty Murray (D-WA)	senator_murray@murray.senate.gov	(202) 224-2621

Senator Murray was a co-sponsor of the "Internet School Filtering Act" of 1998. She also proposed legislation in 1997 that would have made it a crime to rate a site incorrectly.		
Representative Ernest J. Istook (R-OZ)	istook@mail.house.gov	(202) 224-2621
Representative Istook sponsored the Child Protection Act of 1998, the House equivalent of Senator McCain's Internet School Filtering Act. Istook's bill passed the House but was not included in the final 1998 spending bill.		

Deadline a few days from now
Everything above, and then some:

Web sites about blocking software:

- Our blocking software FAQ
- Censorware.Net -- includes reports on some of the sites that have been blocked by WebSENSE, Cyber Patrol, and SmartFilter. Other reports include a revelation that a federal court system used WebSENSE blocking software for its employees, including judges.
- Electronic Privacy Information Center Censorware Page
- TIFAP: The Internet Filter Assessment Project. The results of Karen Schneider's survey of several hundred librarians' experiences with blocking software in test scenarios.

Policy papers written by different organizations analyzing blocking software:

- Access Denied: An Impact of Filtering Software on the Gay and Lesbian Community. From the Gay and Lesbian Alliance Against Defamation, a report on targeting of gay rights Web pages by blocking software companies, and the effects on gay and lesbian children.
- Fahrenheit 451.2: Is Cyberspace Burning? First white paper from the ACLU criticizing blocking software.
- Censorship In A Box. A follow-up report on blocking software from the ACLU.
- Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet, from the Electronic Privacy Information Center.

Another long list of useful links can be found at the Internet Free Expression Alliance Web site.

Resources for journalists writing sensationalist articles

We have sensationalist quotes available for sale according to the following price sheet. If you need a quote to add to your story for dramatic effect, about the dangers of the Internet and the threat that it poses to parents' rights, you can purchase one or more of these quotes and attribute them to "Peacefire" or to a Peacefire representative willing to have themselves quoted.

Story lead	Suggested quote	Price

An activist group wants the local library to be prosecuted for not censoring children's Internet access, claiming that exposure to sexual materials promotes rape and other sex crimes.	"Many other first-world democracies have much less stringent censorship laws, and their sex-crime rates are vastly lower than in the U.S."	**$50**
Father discovers that his daughter has figured out how to use encryption to stop him from reading her e-mail; demands that the authors of the encryption program tell him how to break the encryption, even though this is mathematically impossible.	"The laws of mathematics don't change just because parents want them to change."	**$75**
Parents are furious to discover that their child signed up with a HotMail account in order to send and receive private e-mail; they demand that HotMail set up an age-verification scheme and obtain parental permission before setting up e-mail accounts for minors.	"You can't expect HotMail to spend millions of dollars overhauling their system just to accomodate a few parents who don't want their kids to have any privacy."	**$125**

How to disable your blocking software

If you're in a setting where your actions cannot be traced back to *you personally* -- for example, if you're using a school or cybercafe computer where you don't have to sign in individually, or you're using a home computer where the administrator never checks the logs of what you accessed -- you can try using this site:
http://www.StupidCensorship.com/
That site is of course well known (having been publicized on this page), which is why you should not use it if you are being individually tracked. And of course since the site is well known, it may be blocked already, but there are lots of computers with blocking software installed where the admins are not bothering to update the blocked-site lists any more, so it might work.

If that does not work, then:

Ask a friend to install a "circumventor" Web site on their home machine, using these instructions. The instructions can be followed by most people with a reasonable amount of computer experience (i.e. if they have installed and uninstalled software before).

Once they have completed the instructions, they can give you a URL that you can connect to, which will disable the blocking software on your computer.

Additional instructions for specific programs (currently nothing specific, but more info will be added as necessary):
Bess | Websense | 8e6 | SmartFilter | SonicWall | SurfControl | Cybersitter | Net Nanny | Cyber Patrol

PEACEFIRE
Open Access for the Net Generation

Blocked Site of the Day

Blocking Software Reports

BESS
Cyber Patrol
WebSENSE
Net Nanny
SmartFilter
X-Stop / 8e6
I-Gear
CYBERsitter

About Peacefire
Join Peacefire
Blocking Software FAQ
Contact
Press information

webmaster@
peacefire.org

Home | About Peacefire | Censorware | Contact

Why we do this

What should be the minimum age to get a library card without a parent's signature? How old should you have to be to get medical care without your parents' consent? At what age should your parents no longer be allowed to pull you out of sex education classes at school, or even pull you out of the whole school? I think that most people have never thought seriously about the answers to these questions.

Some people's answer to all of these is, "18, because lots of other people think so." This is usually phrased in fancier language -- "We as a society have determined", "Our civilization has decided", etc. -- but those are really just different ways of saying "Lots of other people think so." The problem with this is that if you defend your beliefs by merely agreeing with people around you, that leads down some bizarre paths. Suppose you live in a state where it's illegal for minors to get an abortion without parental permission, and you support that law. Then you move to a state where abortion for minors is legal. Do you now change your beliefs because you moved? If you're an American woman and you move to Saudi Arabia, do you forget that you ever had any "beliefs", and start trying to forget how to read? It's one thing to say that you should follow the laws of the country or state that you live in, but hopefully you wouldn't change your own personal *views* depending on where you lived, if your views mean anything to you at all. Or to put it another way, if your answer to some question is "lots of other people think so", the obvious question is, "Why do *you* agree with them?"

Why, for example, don't minors have the right -- from, say, age 13 onward -- to read whatever books and watch whatever movies they want? Not because they can't handle it -- in practice, most teenagers are allowed to read and watch whatever they want, and they turn out fine. In that case, is there any reason why it shouldn't be a right for all of them, instead of just the ones whose parents are cool?

Yes, it's true that teenagers don't pay a lot of taxes and are usually freeloading off their parents. But that's not because teenagers are lazy or dumb, it's because they're forced to work all day in school for free. If you took a bus driver's license away and made him study Biology and American History for 10 hours a day, he'd have to move back in with his parents too. This is not to say that school is a waste of time; on the contrary, the whole point of school is that you're investing in yourself, just like a building company owner is investing for the future when they start constructing a new apartment complex. The huge difference, though, is that the building company owner is allowed to enjoy the fruits of their investment right away (getting paid a company salary while the apartments are still being built), but students aren't allowed to get paid while they're investing in themselves. So students may have to live off their parents, but that's only because they're forced to work without getting paid for their investment in themselves, which is hardly their fault. Besides, there are other people -- trophy wives, the homeless, some college students, and various overlaps between those groups -- who really *are* freeloading off of other people and not directly paying taxes, and hardly anyone argues for taking their civil rights away. So if that's not the real reason for most restrictions on minors' rights, then are there other reasons?

For example, it's probably a good thing that parents have the right to stop their five-year-old kids from watching gory movies, because they would give the kids nightmares -- that's an actual *reason*, which is why you rarely see lawyers arguing in court for the First Amendment rights of five-year-olds to rent *Saw III*. On the other hand, studies show that letting parents veto sex education in schools, increases the risk of teenagers having sex for the first time without protection, which would be a strong argument for treating students' access to sex education as a basic right. Perhaps you might find an argument in the other direction -- maybe students who have more sex (even safe sex) get less studying done. (I don't know if any studies show that, but in that case, I would ask if adults who have more sex also get less work done -- and in both cases, whether the tradeoff isn't worth it anyway.) The point is to try and figure out where to draw the line, by weighing the pros and cons of drawing the line at different ages, instead of just saying, "Minors shouldn't have any say until they're 18, because it's always been that way."

Some other examples: the FAA doesn't let passengers under 15 sit in the exit row of an airplane. This is probably a reasonable rule since (a) they picked 15, which has no legal significance, so they must have thought that really was the appropriate age, and (b) it is not a big deal to be asked to move out of the exit row on a plane. On the other hand, most libraries won't give you a library card if you're under 18 without your parents' signature. Is there a real reason for that? Librarians say it's because without a parent's signature, the library can't collect on the money that a minor owes them if the minor loses a book. But couldn't minors just put down a cash deposit for whatever book they're checking out, and get it back when they return it? Besides, if the law doesn't let libraries collect debts from minors, isn't *that* the law that should be changed?

If you want to know whether minors can handle a particular right, like the right to read whatever books and watch whatever movies they want, why not just look at how people under 18 handle it already? Can minors handle the responsibility for their own library cards? Why not just ask the ones who already have one? Or, if you had told people 15 years ago that someday there would be a global computer network that kids could use to access ALL THE PORN IN THE WORLD right from their OWN HOUSE, many people would have been horrified. Now that it's been around for 10 years, there's no evidence that it has affected kids' well-being -- so having a "debate" about whether people under 18 can handle being on the Internet, is a bit silly at this point, because we already know that they can.

On the other hand, some moral questions can't be answered by studies. Take a controversial topic like abortion for minors without parental consent. Now, as for the morality of abortion itself, this seems to me like an unanswerable question -- if you believe that killing a 1-year-old child is murder, but using contraception is not, that means somewhere in between those two points you have to draw the line where you think "murder" begins, and no matter where you draw it, someone could ask why you don't move it a week earlier or a week later. But surely, whether it's murder or not, doesn't depend on whether you have your parents' permission! I remember a Christian Coalition press release about a state's new parental consent law which said, "The decision to terminate a pregnancy -- and indeed a life -- should not be made without parental involvement." It's probably safe to say that whoever wrote that sentence didn't actually mean what it said -- that the decision to "end a life" is OK if your parents sign off on it? I guess that means that if you get arrested for shooting a convenience store clerk, you'd better have that note from your Mom. Abortion in a given situation is either right or wrong, but it's absurd to say that it's only wrong *if* you're under 18 and your parents object.

I don't have final answers to any of these questions, but the point is to spark discussion of civil rights for minors in terms of benefits, drawbacks, evidence, and reasons other than "We've always done it that way." Personally I think that if we followed these principles, then all students would be able to get accurate sex education, responsible teenagers would be able to get their own bank accounts, abortion rights would not depend on age, and everybody would have their own library card. You might argue for different conclusions. But at least weighing the pros and cons gives some framework to the discussion that allows it to get somewhere.

- *Bennett*

How to install the Circumventor program, which gets around all Web-blocking software

Bennett Haselton

This page describes how to install the "Circumventor" program, which can be used to get around all Web blocking programs.

However, **Please Note!!** You don't actually install the Circumventor *on* the computer that is blocked from accessing Web sites. You, or a friend of yours, has to install the Circumventor on some *other* machine which is not censored.

For example, if you want to get around Web blocking at work, don't install the Circumventor on your work computer. Install the Circumventor on your *home* computer. When the installer is done, it will give you the URL for your new Circumventor, and then you write that URL down and take it in with you to work, where you can use that URL to bypass the Web blocking there. Similarly, if you're in China and blocked from accessing certain sites, don't install the Circumventor on a machine in China; instead, get a friend to install it outside China, and then they can send you the URL that you can use to access banned sites.

If you want to, please enter your email address below if you would like to receive updates about the Circumventor software. This will include announcements about new versions and improvements. We will never share your email address with any third party.

Enter your email address:

[Sign up]

How to install the Circumventor

The machine where you install the Circumventor must have a fast Internet connection (not dial-up), and it must be running Windows XP or 2000 (this includes most computers these days). Also, once you install the Circumventor on your machine, the Circumventor **will only work as long as you have your machine turned on and connected to the Internet**, so you should only install it on machines that are online more or less all the time.

NOTE: By installing this software, you will be joining an interconnected Web of Circumventor machines, so just as you can surf the Web via other people's machines (at sites like StupidCensorship.com), at times other users will be surfing the Web through your machine. However, they will not have access to any files or programs on your machine.

To install:

1. Download ActivePerl from this link and install it. It **must** be installed to **C:\Perl** (this should be the default). Accept all of the default options.
2. Download OpenSA 2.0.2 beta from this link (FireFox users -- please right-click and pick "Save Link As") and install it. Accept all of the default options. (If you get to a screen titled "Server Information" and it doesn't have values filled in for "Network Domain", "Server Name" and "Administrator's Email Address", just fill in these boxes with made-up random values -- the Circumventor doesn't use them.)

3. Download the **circumventor-setup.exe** program from this link and pick "Save" -- then once you have saved it on your computer, run the circumventor-setup.exe file that you saved.

If the **circumventor-setup.exe** program succeeds, it will display an "It's ready!" page at the end of the install. If it fails, it will create a file circumventor-setup-log.txt -- send that file to bennett@peacefire.org and we will try to figure out what went wrong.

Happy surfing!

Special thanks

This project was made possible by the existence of the following programs, which are generously given away for free by their authors:

- OpenSA, the Open Server Architecture project, by Daniel Reichenbach -- the Web server that encrypts communications traffic and forms the backbone of the Circumventor.
- CGIProxy by James Marshall -- the CGI script which fetches blocked Web pages.
- Windows NT/2000/XP Utilities by Luis Carlos Castro Skertchly.
- Perl by Larry Wall.

Exhibit B

HONORABLE ROBERT S. LASNIK

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

BENNETT HASELTON, an individual; PEACEFIRE, INC., a Washington corporation Plaintiff, vs. QUICKEN LOANS, INC., a Michigan corporation; and JOHN DOES, I-X Defendant.	CIVIL ACTION NO. C07-1777 RSL **DEFENDANT QUICKEN LOANS INC.'S FIRST INTERROGATORIES AND REQUESTS FOR PRODUCTION TO PLAINTIFFS** **AND RESPONSES**

TO: Plaintiff Bennett Haselton and to Peacefire, Inc.

AND TO: Robert J. Siegel, his attorney

I. INSTRUCTIONS

1. Pursuant to FRCR 33, you shall serve the answers to all interrogatories and any and all objections within 30 days after service, upon Dorsey & Whitney LLP, U.S. Bank Building Center, 1420 Fifth Avenue, Suite 3400, Seattle, Washington, attorneys for Defendant Quicken Loans Inc.

2. You must answer each interrogatory on the basis of your entire knowledge. You must furnish all requested information that is known by, possessed by, or available to you or any of your attorneys, health care providers, consultants, representatives, or other agents.

INTERROGATORY NO. 4: Please identify each and every web-hosting service, internet service provider, or other provider of online services from whom you have purchased, leased or otherwise obtained services in relation to your operation of the "Peacefire.org" domain.

ANSWER:

The Peacefire.org domain and virtual Web server are hosted by JVDS, Inc. at www.jvds.com.

REQUEST FOR PRODUCTION NO. 2: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

We have no physical written contract with JVDS. We signed up for hosting at their Web site at www.jvds.com.

INTERROGATORY NO. 5: Please identify any programs, software, or other system used by you to prevent or reduce the receipt of unsolicited commercial e-mail.

ANSWER:

Whenever I have tested a "spam filter", or had a spam filter activated without my knowledge by my ISP, it has blocked a significant number of legitimate e-mail messages, which imposed more costs on me than the savings resulting from the spam being blocked. For this reason we do not use any spam filtering.

REQUEST FOR PRODUCTION NO. 3: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

None

previously had with website hosting services, Internet service providers or other providers of online services in relation to your use of the domain name Peacefire.org from 2005 to present.

RESPONSE: Same as Request For Production #2.

INTERROGATORY NO. 9: Please identify any service you provide that enables users to access content, information, electronic mail, or other services offered over the internet, and for each such service, please identify the users to whom you provide that service (including their address, e-mail and phone number), the nature of the service, and the consideration paid for the service from 2005 to the present.

ANSWER: Objection: Relevance. This information is not relevant, is not reasonably calculated to lead to the discovery of admissible evidence, and is interposed solely to intimidate and harass. Regardless of whether Peacefire has numerous, or no subscribers, it still qualifies as an Interactive Access Service ("IAS") under the definition used in the Can-Spam Act. Peacefire intends to move the Court for a protective order to protect the identities of its subscribers.

/s/ Robert J. Siegel
Robert J. Siegel, WSBA #17312

Notwithstanding the foregoing objections, Peacefire responds as follows:

Peacefire currently has a mailing list of about 90,000 subscribers to whom Peacefire sends out information and notifications of new proxies to carry their traffic. To protect users' privacy we do not ask for this information at the time that they sign up. However, judging from the e-mails that I receive requesting help with the sites, a significant portion of subscribers reside in heavily censored countries, and their lives and liberty could be at serious risk were their identities to be disclosed. For this reason, we decline to provide the identities of our subscribers.

This internet access service had its genesis in a project begun in 2002 for the International Broadcasting Bureau in Washington D.C. (better known under the name of their most famous project, Voice of America). Attached are true and correct copies of some of the invoices and work orders for this project.

One of Voice of America's primary missions is to counter anti-American government sponsored propaganda in totalitarian and repressive regimes.

To further that mission, Voice of America contracted with Peacefire to create systems to allow citizens of repressive governments, such as China and Iran, to circumvent their government's censorship of the internet.

These systems included software called "the Circumventor" program and servers set up to run the Circumventor program.

In 2003 Peacefire released the first version of the Circumventor program under the Voice of America contract.

While the Voice of America contract has been completed, Peacefire continues to operate the Circumventor program with the full knowledge and blessing of the United States Government's International Broadcasting Bureau in Washington D.C.

Peacefire currently maintains several Internet access proxies running versions of this program to assist users in getting around censorship.

Since the contract with Voice of America expired, Peacefire has paid for ongoing operations and machine maintenance by running advertising on the machines running the Circumventors that users use to access Web sites from censored countries. There are very few Internet Access services of this kind in the world, so Peacefire subscribers living under repressive governments throughout the world are heavily dependent on Peacefire for this service.

To provide Internet access services to our users, we lease 22 dedicated proxy servers around the U.S., which we use to create new "proxy sites" to carry our subscribers' traffic. Our total expenses for computer services in 2007 were $39,035 and our total expenses of all kinds from operating the business came to $47,395.

Our user database is hosted on our server, and we send communications to our subscribers and connect them with newly set up proxy servers, using custom scripts that we have written ourselves.

To obtain a report of how many subscribers we have at any given time, we run the following command while logged in to the system:

```
mysql> select count(*) from circumventor_newsletter_subscriber where
has_confirmed;
+----------+
| count(*) |
+----------+
|   93202 |
+----------+
```

The above number of 93,202 is the most recent subscriber number obtained on March 18, 2008.

We don't know what proportion of these users are in different countries such as Iran and China, since their e-mail addresses do not reveal this (many of them use Yahoo and Hotmail addresses), and we cannot tell from the IP address that they used to sign up either (if they used a proxy to access our site, that would hide the IP address they used to sign up).

REQUEST FOR PRODUCTION NO. 6: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

See Objection to preceding Interrogatory, which is reiterated, and hereby incorporated here.

Notwithstanding the foregoing objections, Plaintiff responds as follows:

Copies of our contract with Voice of America are attached.

INTERROGATORY NO. 10: With respect to your claim for damages in this case, for each and every claim alleged, please state the damages you seek thereunder and specifically include a computation of each such category of damages and identify the basis upon which you claim such damages are available thereunder.

ANSWER:

Defendants initiated the transmission of the E-mails, and each of them, to a protected computer in violation of 15 U.S.C. §7704(a), causing damage to Plaintiff Peacefire as the provider of the Internet access service receiving each such E-mail in the amount of $100 for each such E-mail, as provided in 15 U.S.C. §7706 (g) (3).

Defendants initiated, conspired with another to initiate, or assisted the transmission of the E-mails, and each of them, in violation of RCW 19.190.020, causing damage to Plaintiffs Peacefire and Haselton as the interactive computer services receiving each such E-mail in the amount of $1,000 for each such E-mail, and to Plaintiff Haselton individually in the amount of $500 for each such E-mail directed to and received at Haselton's E-mail address, as provided in RCW 19.190.040(1) and (2).

Defendants initiated the E-mails, and each of them, in violation of RCW 19.190.030 and Chapter 19.86 RCW, causing damage to Plaintiffs as the recipients of each such E-mail in an amount to be proven at trial, including, but not limited to, treble damages. Defendants' acts as described hereinabove constituted unfair and deceptive acts or practices in the conduct of trade or commerce, which acts or practices caused injury to Plaintiffs, and as such constitute independent violations of RCW 19.86 et seq.

Although actual damages in the way of costs incurred to monitor and control spam, and for time expended to monitor, control, and manage spam have been incurred, these are difficult to calculate precisely. Nonetheless, Plaintiffs will endeavor to calculate such damages for purposes of trial.

Also See Answer to Interrogatory No. 11 below.

REQUEST FOR PRODUCTION NO. 7: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

To be produced at a later date.

INTERROGATORY NO. 11: Please identify the "harm" you suffered as a result of receiving the AOM.

ANSWER:

1. We currently receive about 10,000 spams per week from mostly unidentified sources (in addition to the several hundred legitimate mails per week that we must read and respond). The amount of spam that we receive directly impedes the responsiveness of our server and our ability to communicate with our subscribers to send them the locations of new proxy servers. At a typical moment during business hours, there are about 100 instances of the "sendmail" program running on the www.peacefire.org server, each of which is triggered by a remote server sending us mail, the vast majority of which is currently spam.

2. Each instance of sendmail or spam consumes CPU and memory resources. We have tried to combat the problem by buying more memory for the Peacefire.org server, but since mail-handling programs use a queue to prioritize and send mail, the amount of spam that we receive continues to impact us regardless of what hardware upgrades we buy. As a result, the mail that we attempt to send to our subscribers, and the mail that business contacts attempt to send us, is sent more slowly, with random delays, and sometimes does not get sent at all. While the hosting cost for the www.peacefire.org

site is small compared to the cost of our proxy servers, when we are impeded from sending mail to our subscribers, that means that a substantial portion of the hosting costs we've paid for our proxy servers is going to waste.

3. We have publicly advocated the development of better spam filters as an alternative to litigation for fighting spam. Unfortunately, the existing spam filters on the market are not accurate enough to make them a viable alternative for companies in our position who cannot afford to miss business-critical mails. Every time we have purchased and tried using a filter to reduce the impact of spam on our system, it has ended up blocking so much legitimate mail that the interference with our business made it impractical to keep using the filter. In one instance, an ISP's spam filter resulted in all mail being blocked that was forwarded from one of our sub-businesses (tracerlock.com), resulting in all customer communications over several hours being lost before we found out what was happening. Other lost mails have included business-critical communications from advertisers and business clients.

4. Our mail is especially vulnerable because we receive mail from places such as China and India that are frequently blacklisted by spam filters.

5. Spam filters have gained acceptance because they work well for casual users who do not mind if mail is sometimes blocked, or who only exchange mail with a small number of legitimate business-critical contacts (so they can add all of those contacts to their filter's exceptions list), but neither of those circumstances apply to us. In general, spam filters block far more legitimate mail than the general public realizes. (Both Hotmail and AOL, for example, have announced that senders will have to pay fees in order to bypass their companies' spam filters, or risk being blocked as spam. This means that the mails which end up caught by their "spam filters" will not in all cases truly be spam, but could be email sent by any company which didn't pay the white-list fee.)

6. There are also other impacts and expenses associated with receiving so much spam, including the loss of productive time spent filtering and deleting it, and the

consequences of accidentally deleting legitimate messages along with the spam. In one instance, I accidentally deleted a mail from an advertiser who was disputing part of an earnings report, and because I didn't respond within two days, they suspended their relationship with us for about the next three weeks, costing us about $4,000 in lost revenue. If I hadn't deleted the message along with all the spam that I received that day, the dispute might have been averted and the loss of revenue avoided.

7. In April 2007 we upgraded our RAM from 64 MB to 256 MB which costs an extra $26.50/month in order to deal with the high volume of spam. While this may not seem like a large expense, in relation to our overall income, even small costs like this become significant.

REQUEST FOR PRODUCTION NO. 8: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

See attached documents.

INTERROGATORY NO. 12: Please identify each source of "revenue" you have received during the past five years.

ANSWER:

Tax returns for years falling within that period have been attached.

REQUEST FOR PRODUCTION NO. 9: Please produce any and all documents that refer or relate to your response to the preceding interrogatory.

RESPONSE:

See attached tax returns.

REQUEST FOR PRODUCTION NO. 10: Please provide the phone records for phone number 206-279-8164 from June 1, 2005 through July 30, 2005.